

【書類名】 特許願

【整理番号】 A009904769

【提出日】 平成11年 8月31日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 7/00

【発明の名称】 拡大鍵生成装置、暗復号装置及び記憶媒体

【請求項の数】 20

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 大森 基司

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 横田 薫

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 関部 勉

【発明者】

 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

 【氏名】 館林 誠

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

 【氏名】 佐野 文彦

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

【氏名】 川村 信一

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705037

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 拡大鍵生成装置、暗復号装置及び記憶媒体

【特許請求の範囲】

【請求項 1】 各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置であって、

前記各鍵変換関数部は、

前記入力された鍵から得られた第 1 鍵に基づいて所定の置換テーブルにより変換処理を行う第 1 鍵変換手段と、

この第 1 鍵変換手段による変換結果と前記入力された鍵から得られた第 2 鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段と

を備えたことを特徴とする拡大鍵生成装置。

【請求項 2】 請求項 1 に記載の拡大鍵生成装置において、

前記各鍵変換関数部は、

入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段を備えたことを特徴とする拡大鍵生成装置。

【請求項 3】 請求項 2 に記載の拡大鍵生成装置において、

前記巡回シフト手段のシフト量は、前記第 1 鍵変換手段の出力ビット数と互いに素な値であることを特徴とする拡大鍵生成装置。

【請求項 4】 請求項 1 に記載の拡大鍵生成装置において、

前記各鍵変換関数部は、

入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段を備えたことを特徴とする拡大鍵生成装置。

【請求項 5】 請求項 1 乃至請求項 4 のいずれか 1 項に記載の拡大鍵生成装置において、

前記各鍵変換関数部は、

前記第 1 鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入

力する拡大変換手段を備えたことを特徴とする拡大鍵生成装置。

【請求項 6】 請求項 5 に記載の拡大鍵生成装置において、

前記拡大変換手段による拡大変換は、所定ビット数のシフトであることを特徴とする拡大鍵生成装置。

【請求項 7】 請求項 1 乃至請求項 6 のいずれか 1 項に記載の拡大鍵生成装置において、

前記拡大鍵演算手段による演算は、桁上りを伴う加算であることを特徴とする拡大鍵生成装置。

【請求項 8】 請求項 1 乃至請求項 7 のいずれか 1 項に記載の拡大鍵生成装置を備えた暗復号装置において、

前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部を備えたことを特徴とする暗復号装置。

【請求項 9】 請求項 8 に記載の暗復号装置において、

前記攪拌部は、前記暗号化及び前記復号のための複数の置換テーブルを有し、前記攪拌部のいずれかの置換テーブルは、前記第 1 鍵変換手段の置換テーブルと共有化されていることを特徴とする暗復号装置。

【請求項 10】 請求項 9 に記載の暗復号装置において、

前記各鍵変換関数部は、

前記第 1 鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手段に入力する拡大変換手段を備えたことを特徴とする暗復号装置。

【請求項 11】 各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置に使用されるコンピュータ読み取り可能な記憶媒体であって、

前記拡大鍵生成装置内のコンピュータに、

前記各鍵変換関数部として、

前記入力された鍵から得られた第 1 鍵に基づいて所定の置換テーブルにより変

換処理を行う第 1 鍵変換手段、

この第 1 鍵変換手段による変換結果と前記入力された鍵から得られた第 2 鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 1 2】 請求項 1 1 に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 1 3】 請求項 1 2 に記載のコンピュータ読み取り可能な記憶媒体において、

前記巡回シフト手段のシフト量は、前記第 1 鍵変換手段の出力ビット数と互いに素な値であるコンピュータ読み取り可能な記憶媒体。

【請求項 1 4】 請求項 1 1 に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 1 5】 請求項 1 1 乃至請求項 1 4 のいずれか 1 項に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

前記第 1 鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入力する拡大変換手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

体。

【請求項 16】 請求項 15 に記載のコンピュータ読み取り可能な記憶媒体において、

前記拡大変換手段による拡大変換は、所定ビット数のシフトであるコンピュータ読み取り可能な記憶媒体。

【請求項 17】 請求項 11 乃至請求項 16 のいずれか 1 項に記載のコンピュータ読み取り可能な記憶媒体において、

前記拡大鍵演算手段による演算は、桁上りを伴う加算であるコンピュータ読み取り可能な記憶媒体。

【請求項 18】 請求項 11 乃至請求項 17 のいずれか 1 項に記載の拡大鍵生成装置を備えた暗復号装置に使用されるコンピュータ読み取り可能な記憶媒体において、

前記暗復号装置内のコンピュータに、

前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 19】 請求項 18 に記載のコンピュータ読み取り可能な記憶媒体において、

前記攪拌部は、前記暗号化及び前記復号のための複数の置換テーブルを有し、

前記攪拌部のいずれかの置換テーブルは、前記第 1 鍵変換手段の置換テーブルと共有化されているコンピュータ読み取り可能な記憶媒体。

【請求項 20】 請求項 19 に記載のコンピュータ読み取り可能な記憶媒体において、

前記各鍵変換関数部としては、

前記第 1 鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手

段に入力する拡大変換手段、

を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、秘密鍵ブロック暗号に適用される拡大鍵生成装置、暗復号装置及び記憶媒体に関する。

【0002】

【従来の技術】

近年の計算機・通信技術の分野では、送信データを暗号化して送信し、受信データを復号して受信内容を得る暗号技術が広く知られている。この種の暗号技術では、暗号化と復号に同じ秘密鍵（以下、共通鍵という）を用いる暗号化アルゴリズムが共通鍵暗号と呼ばれている。共通鍵暗号では、一般に、入力メッセージが固定長の入力ブロックに分割され、各ブロックが鍵に基づいて攪拌処理され、暗号文が生成されている。係る共通鍵暗号としては、例えばDES（データ暗号化規格：data encryption standard）と呼ばれる方式が広く用いられている。

【0003】

DES方式による暗号化では、図15（a）に示すように、平文に初期転置 IP を施したデータに対し、ラウンド関数による処理を16回施す。さらにラウンド関数処理されたデータに初期転置の逆転置 IP^{-1} を施すことで暗号文を得ている。また、各ラウンド関数に対し、元の鍵から生成される拡大鍵を与えることでラウンド関数における処理が実行される。

【0004】

つまり、DES方式による暗号化装置は、多数のラウンド関数によって暗号化対象となるデータを攪拌する攪拌部と、攪拌部の各ラウンド関数に拡大鍵を与える鍵生成部をその主要構成としている。

【0005】

一方、DES方式による復号は、図15（b）に示すように、暗号化時とは逆

の順番で復号対象のデータにラウンド関数の処理を施す。従って、鍵生成部からの拡大鍵も、暗号化時の最後のラウンド関数で使用されたものから順番に生成する。

【 0 0 0 6 】

このDES方式における第1の利点は、暗号化回路と復号回路の大半を共通化可能な構成にある。つまり、図15(a)，図15(b)に示すように、攪拌部のラウンド関数は、暗号化時と復号時とでは拡大鍵の入力順序は逆になるが、同一の回路が使用される。

【 0 0 0 7 】

DES方式の第2の利点は、1つの共通鍵を用いて暗号化と復号とを行うため、管理対象の鍵が少ないことである。なお、DES方式では、唯一の共通鍵に基づいて拡大鍵を逆順に生成するため、鍵生成部では次の処理を行っている。

【 0 0 0 8 】

すなわち、暗号化の際には、共通鍵を左巡回シフト（左ローテート）し、各拡大鍵を生成する。なお、巡回シフト量の合計値を共通鍵のビット数に定め、最終段で中間的な鍵が初期状態（共通鍵）に戻される。これにより、暗号化時の最後の拡大鍵と復号時の最初の拡大鍵とを同一の値に生成し得る。復号時には、共通鍵を逆に右巡回シフト（右ローテート）して逆順に各拡大鍵を生成すればよい。

【 0 0 0 9 】

しかしながら、DES方式では、鍵生成部の処理が転置処理のみで構成されるため、一般に弱鍵（weak key）と呼ばれる安全性の低い鍵が存在するという問題がある。なお、弱鍵は、本明細書中、互いに同一な拡大鍵を意味しており、全ての拡大鍵 $K_1 \sim K_{16}$ が互いに同一な場合（ $K_1 = K_2 = \dots = K_{16}$ ）と、半分の拡大鍵 $K_1 \sim K_8$ ， $K_9 \sim K_{16}$ が互いに同一な場合（ $K_1 = K_{16}$ ， $K_2 = K_{15}$ ， \dots ， $K_8 = K_9$ ）とを含んでいる。

【 0 0 1 0 】

但し、係る弱鍵の生成は、脅威的なものではなく、弱鍵を生成するパターンをもつ共通鍵の入力を除去する装置、あるいは生成された拡大鍵が弱鍵でないか否かを判別し且つ弱鍵のときには除去する装置を付加することにより、十分に阻止

可能であると考えられる。

【0011】

しかしながら、この種の弱鍵の生成阻止に関する装置を付加した場合、拡大鍵生成装置及び暗復号装置の価格を上昇させてしまい、さらに、拡大鍵生成装置及び暗復号装置の規模を増大させる可能性がある。

【0012】

また、DES方式に限らず、弱鍵の生成を阻止することにより、本来の各ラウンド毎に異なる拡大鍵を用いた場合の暗号強度を実現させ、さらに、その暗号強度を向上し得る暗号方式が望まれている。

【0013】

【発明が解決しようとする課題】

以上説明したように従来の拡大鍵生成装置及び暗復号装置では、安全性の低下を阻止する観点から、弱鍵の生成阻止に関する装置を付加すると、拡大鍵生成装置及び暗復号装置の価格を上昇させてしまい、さらに、拡大鍵生成装置及び暗復号装置の規模を増大させる可能性がある。

【0014】

また、弱鍵の生成を阻止しても、鍵生成部の処理が暗号強度の向上にあまり貢献しておらず、暗号強度の向上が望まれている。

【0015】

本発明は上記実情を考慮してなされたもので、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度の向上を図り得る拡大鍵生成装置、暗復号装置及び記憶媒体を提供することを目的とする。

【0016】

【課題を解決するための手段】

請求項1に対応する発明は、各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置であって、前記各鍵変換関数部としては、前記入力された鍵から得られた第1鍵に基づいて所定の置換テーブルにより変換処理を行う第1鍵変換手段と、この第1鍵変換手段による変換結果と前記入力された鍵から得られた第

2 鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段とを備えた拡大鍵生成装置である。

【0 0 1 7】

また、請求項 2 に対応する発明は、請求項 1 に対応する拡大鍵生成装置において、前記各鍵変換関数部としては、入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段を備えた拡大鍵生成装置である。

【0 0 1 8】

さらに、請求項 3 に対応する発明は、請求項 2 に対応する拡大鍵生成装置において、前記巡回シフト手段のシフト量としては、前記第 1 鍵変換手段の出力ビット数と互いに素な値である拡大鍵生成装置である。

【0 0 1 9】

また、請求項 4 に対応する発明は、請求項 1 に対応する拡大鍵生成装置において、前記各鍵変換関数部としては、入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段を備えた拡大鍵生成装置である。

【0 0 2 0】

さらに、請求項 5 に対応する発明は、請求項 1 乃至請求項 4 のいずれか 1 項に対応する拡大鍵生成装置において、前記各鍵変換関数部としては、前記第 1 鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入力する拡大変換手段を備えた拡大鍵生成装置である。

【0 0 2 1】

また、請求項 6 に対応する発明は、請求項 5 に対応する拡大鍵生成装置において、前記拡大変換手段による拡大変換としては、所定ビット数のシフトである拡大鍵生成装置である。

【0 0 2 2】

さらに、請求項 7 に対応する発明は、請求項 1 乃至請求項 6 のいずれか 1 項に対応する拡大鍵生成装置において、前記拡大鍵演算手段による演算としては、桁上りを伴う加算である拡大鍵生成装置である。

【 0 0 2 3 】

また、請求項 8 に対応する発明は、請求項 1 乃至請求項 7 のいずれか 1 項に対応する拡大鍵生成装置を備えた暗復号装置において、前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部を備えた暗復号装置である。

【 0 0 2 4 】

さらに、請求項 9 に対応する発明は、請求項 8 に対応する暗復号装置において、前記攪拌部が、前記暗号化及び前記復号のための複数の置換テーブルを有し、前記攪拌部のいずれかの置換テーブルが、前記第 1 鍵変換手段の置換テーブルと共有化されている暗復号装置である。

【 0 0 2 5 】

また、請求項 1 0 に対応する発明は、請求項 9 に対応する暗復号装置において、前記各鍵変換関数部としては、前記第 1 鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手段に入力する拡大変換手段を備えた暗復号装置である。

【 0 0 2 6 】

さらに、請求項 1 1 に対応する発明は、各ラウンド毎に異なる鍵が入力され、それぞれ前記鍵に基づいて拡大鍵を生成する複数の鍵変換関数部がカスケードに連結された拡大鍵生成装置に使用されるコンピュータ読み取り可能な記憶媒体であって、前記拡大鍵生成装置内のコンピュータに、前記各鍵変換関数部として、前記入力された鍵から得られた第 1 鍵に基づいて所定の置換テーブルにより変換処理を行う第 1 鍵変換手段、この第 1 鍵変換手段による変換結果と前記入力された鍵から得られた第 2 鍵とに基づいて前記拡大鍵を算出する拡大鍵算出手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【 0 0 2 7 】

また、請求項 1 2 に対応する発明は、請求項 1 1 に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、入力された鍵を左又は右に巡回シフトさせ、前記巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力する巡回シフト手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【 0 0 2 8 】

さらに、請求項 1 3 に対応する発明は、請求項 1 2 に対応するコンピュータ読み取り可能な記憶媒体において、前記巡回シフト手段のシフト量が、前記第 1 鍵変換手段の出力ビット数と互いに素な値であるコンピュータ読み取り可能な記憶媒体である。

【 0 0 2 9 】

また、請求項 1 4 に対応する発明は、請求項 1 1 に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力する入力鍵変換手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【 0 0 3 0 】

さらに、請求項 1 5 に対応する発明は、請求項 1 1 乃至請求項 1 4 のいずれか 1 項に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、前記第 1 鍵変換手段による変換結果を拡大変換させて前記拡大鍵算出手段に入力する拡大変換手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【 0 0 3 1 】

また、請求項 1 6 に対応する発明は、請求項 1 5 に対応するコンピュータ読み取り可能な記憶媒体において、前記拡大変換手段による拡大変換としては、所定ビット数のシフトであるコンピュータ読み取り可能な記憶媒体である。

【 0 0 3 2 】

さらに、請求項 1 7 に対応する発明は、請求項 1 1 乃至請求項 1 6 のいずれか 1 項に対応するコンピュータ読み取り可能な記憶媒体において、前記拡大鍵演算

手段による演算が、桁上りを伴う加算であるコンピュータ読み取り可能な記憶媒体である。

【0033】

また、請求項 18 に対応する発明は、請求項 11 乃至請求項 17 のいずれか 1 項に対応する拡大鍵生成装置を備えた暗復号装置に使用されるコンピュータ読み取り可能な記憶媒体において、前記暗復号装置内のコンピュータに、前記各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力する攪拌部、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0034】

さらに、請求項 19 に対応する発明は、請求項 18 に対応するコンピュータ読み取り可能な記憶媒体において、前記攪拌部が、前記暗号化及び前記復号のための複数の置換テーブルを有し、前記攪拌部のいずれかの置換テーブルが、前記第 1 鍵変換手段の置換テーブルと共有化されているコンピュータ読み取り可能な記憶媒体である。

【0035】

また、請求項 20 に対応する発明は、請求項 19 に対応するコンピュータ読み取り可能な記憶媒体において、前記各鍵変換関数部としては、前記第 1 鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは前記半分のビット数に前記変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて前記拡大鍵算出手段に入力する拡大変換手段、を実現させるためのプログラムを記憶したコンピュータ読み取り可能な記憶媒体である。

【0036】

(作用)

従って、請求項 1, 11 に対応する発明は以上のような手段を講じたことにより、各鍵変換関数部としては、第 1 鍵変換手段が、入力された鍵から得られた第 1 鍵に基づいて所定の置換テーブルにより変換処理を行い、拡大鍵算出手段が、

この第 1 鍵変換手段による変換結果と入力された鍵から得られた第 2 鍵とに基づいて拡大鍵を算出する。

【 0 0 3 7 】

このように、外部装置を付加しない簡易な構成を用いており、拡大鍵を生成する際に、置換テーブルによる非線形変換処理を行うため、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度を向上させることができる。

【 0 0 3 8 】

また、請求項 2，1 2 に対応する発明は、各鍵変換関数部としては、巡回シフト手段が、入力された鍵を左又は右に巡回シフトさせ、巡回シフトの完了した鍵を次ラウンドの鍵変換関数部に入力するので、請求項 1，1 1 に対応する作用に加え、容易且つ確実に、各ラウンドに入力される鍵を互いに相違させることができる。

【 0 0 3 9 】

さらに、請求項 3，1 3 に対応する発明は、巡回シフト手段のシフト量としては、第 1 鍵変換手段の出力ビット数と互いに素な値であるので、各ラウンドにおけるほぼ全ての第 1 鍵を互いに相違させることができ、請求項 2，1 2 に対応する作用をより一層、容易且つ確実に奏することができる。

【 0 0 4 0 】

また、請求項 4，1 4 に対応する発明は、各鍵変換関数部としては、入力鍵変換手段が、入力された鍵を置換テーブルにより変換し、この変換の完了した鍵を次ラウンドの鍵変換関数部に入力するので、請求項 1，1 1 に対応する作用に加え、容易且つ確実に、各ラウンドに入力される鍵を互いに相違させることができる。

【 0 0 4 1 】

さらに、請求項 5，1 5 に対応する発明は、各鍵変換関数部としては、拡大変換手段が、第 1 鍵変換手段による変換結果を拡大変換させて拡大鍵算出手段に入力するので、請求項 1～4，1 1～1 4 のいずれかに対応する作用に加え、第 1 鍵の攪拌作用を拡大鍵の任意の領域に反映させることができる。

【0 0 4 2】

また、請求項 6， 1 6 に対応する発明は、拡大変換手段による拡大変換としては、所定ビット数のシフトであるので、請求項 5， 1 5 に対応する作用を容易且つ確実に奏することができる。

【0 0 4 3】

さらに、請求項 7， 1 7 に対応する発明は、拡大鍵演算手段による演算としては、桁上りを伴う加算であるので、請求項 1～6， 1 1～1 6 のいずれかに対応する作用を、容易且つ確実に奏することができる。

【0 0 4 4】

また、請求項 8， 1 8 に対応する発明は、攪拌部が、各鍵変換関数部により生成された各拡大鍵に基づいて、入力された平文を暗号化して暗号文を出力し、且つ、入力された暗号文を復号して平文を出力するので、請求項 1～7， 1 1～1 7 のいずれかに対応する拡大鍵生成装置を備えた暗復号装置を実現することができる。

【0 0 4 5】

さらに、請求項 9， 1 9 に対応する発明は、攪拌部が、暗号化及び復号のための複数の置換テーブルを有し、攪拌部のいずれかの置換テーブルが、第 1 鍵変換手段の置換テーブルと共有化されているので、請求項 8， 1 8 に対応する作用に加え、装置規模の縮小化を図ることができる。

【0 0 4 6】

また、請求項 1 0， 2 0 に対応する発明は、各鍵変換関数部としては、拡大変換手段が、第 1 鍵変換手段による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは半分のビット数に変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて拡大鍵算出手段に入力するので、請求項 9， 1 9 に対応する作用に加え、第 1 鍵の攪拌作用を拡大鍵にて左シフトさせた領域に反映させることができ、この場合、攪拌部の複数の置換テーブルに入力される領域に反映させることができるので、より一層、暗号強度の向上を図ることができる。

【0 0 4 7】

【発明の実施の形態】

以下、本発明の各実施形態について図面を参照して説明する。

【0048】

(第1の実施形態)

図1は本発明の第1の実施形態に係る暗復号装置の構成を示すブロック図であり、図2はこの暗復号装置内の拡大鍵生成部の構成を示すブロック図である。

【0049】

この暗復号装置は、パーソナルコンピュータやワークステーション等の計算機の暗復号処理部として構成されており、ハードウェア又はソフトウェアによって暗号化処理と復号処理を行うものであって、具体的には、共通鍵から n 段の拡大鍵 $K_1 \sim K_n$ を生成する拡大鍵生成部10と、拡大鍵生成部10により生成された拡大鍵 $K_1 \sim K_n$ を順次各ラウンド $R_1 \sim R_n$ に用いて暗号化又は復号を行う攪拌部20とを備えている。すなわち、拡大鍵生成部10及び攪拌部20は、暗号化と復号に共通して用いられており、ソフトウェアにより暗復号装置を実現する場合には両者の動作を示すプログラムが予め記憶媒体からインストールされている。なお、拡大鍵生成部10及び攪拌部20の間には転置処理等を設けてもよい。

【0050】

ここで、拡大鍵生成部10は、各ラウンド $R_1 \sim R_n$ に対応し、順にカスケード接続された鍵変換関数 $f_{k1} \sim f_{kn}$ （単に鍵変換関数 f_k ともいう）が設けられている。鍵変換関数 $f_{k1} \sim f_{kn}$ は、共通鍵 K_C 若しくは中間的な鍵変換結果 $k_{c1} \sim k_{cn-1}$ が入力されると、これを変換して得られた拡大鍵 $K_1 \sim K_n$ を攪拌部20のラウンド関数 $f_{r1} \sim f_{rn}$ に出力し、また別途得られた中間的な鍵変換関数 $k_{c1} \sim k_{cn-1}$ を次段の鍵変換関数 $f_{k2} \sim f_{kn}$ に入力する機能をもっている。

【0051】

ここで、鍵変換関数 $f_{k1} \sim f_{kn}$ は、図2に示すように、一時鍵レジスタ $11_1 \sim 11_n$ 、定数レジスタ $12_1 \sim 12_n$ 、XOR素子 $13_1 \sim 13_n$ 、Sボックス $14_1 \sim 14_n$ 、拡大変換部 $15_1 \sim 15_n$ 、加算部 $16_1 \sim 16_n$ 及び

巡回シフト部 $17_1 \sim 17_{n-1}$ を備えている。なお、最終段の巡回シフト部 17_n は、次段に鍵変換関数 $f_k(n+1)$ が無く、不要であるため、省略されている。

【0052】

一時鍵レジスタ 11_i (但し、 $1 \leq i \leq n$ 、以下も同様) は、拡大鍵生成部 10 に入力された共通鍵又は前段の鍵変換関数 $f_k(i-1)$ から入力された中間的な鍵変換結果を保持するものであり、ここでは、56ビットのレジスタが使用されている。

【0053】

定数レジスタ 12_i は、鍵変換関数 $f_k i$ の属するラウンド数に対応して定数が設定され、設定値が XOR 素子 13_i から読出可能となっている。具体的には、定数レジスタ 12_i は、ラウンド数 $n=16$ の例を図 3 (a) に示すように、拡大鍵 $K1 \sim K16$ を逆順 ($K16 \sim K1$) にも生成可能な観点から、保持する定数がラウンド数の中央値 ($n=8, 9$) を中心として左右対称 (前段、後段で対称) に設定されている。但し、これに限らず、定数レジスタ 12_i は、拡大鍵 $K1 \sim K16$ を逆順 ($K16 \sim K1$) にも生成可能であれば、保持する定数は任意であり、例えば図 3 (b) に示すように、暗号化と復号の時とで定数を置換しても良い。なお、定数レジスタ 12_i は、保持する定数のうち、少なくともどれか一つの値を他とは異ならせて設定されていれば良い。

【0054】

XOR 素子 13_i は、一時鍵レジスタ 11_i 内の 8 ビットのデータからなる第 1 鍵 KA と、定数レジスタ内の定数との排他的論理和を算出し、得られた 8 ビットの算出結果を S ボックスに入力するものである。

【0055】

S (置換: substitution) ボックス 14_i は、弱鍵 (全ての段で同じ拡大鍵) の生成を阻止するためのものであり、具体的には、XOR 素子 13_i から入力された 8 ビットの値を非線形変換し、得られた 8 ビットの変換結果を拡大変換部 15_i に入力する機能を有し、例えば図 4 に示すように入力ビットと出力ビットとを置換するための置換テーブルが使用可能となっている。例えば、S ボックス 1

4 i では、入力ビットが (0 0 0 0 0 0 0 1) である場合、その (0 0 0 0 0 0 0 1) という情報を 2 進表現であるとみなし、さらにその 2 進表現を 1 0 進表現した値「1」に変換する。

【0 0 5 6】

そして、図 4 の置換テーブルを参照して「1 番目」の要素「5 4」を決定し、その 2 進表現である (0 1 0 1 0 1 0 0) を出力ビットとして出力する。

そのため、入力ビット (0 0 0 0 0 0 0 1) を出力ビット (0 1 0 1 0 1 0 0) に置換することができる。

【0 0 5 7】

なお、上述のように図 4 の置換テーブルは 0 番～2 5 5 番目までの 2 5 6 個の入力に対応した要素を保持しており、0～2 5 5 の値が入力された場合に対応する 0～2 5 5 の値を決定する場合に用いられるものである。

【0 0 5 8】

また、S ボックス 1 4 i は、装置規模の縮小化の観点から、後述するラウンド関数 f k 内のいずれかの S ボックスと共有することが好ましい。

【0 0 5 9】

拡大変換部 1 5 i は、S ボックス 1 4 i から入力された 8 ビットの変換結果を大きな値に変換するものであり、ここでは、8 ビットの変換結果を 4 ビットだけ左シフトさせるように拡大変換し、得られた 1 2 ビットの拡大変換結果を加算部 1 6 i に入力する機能をもっている。

【0 0 6 0】

なお、拡大変換部 1 5 i のシフト量は、S ボックス 1 4 i の出力ビットを後述する攪拌部 2 0 の 2 つの S ボックス S 3, S 4 に反映させる観点から、等価的に S ボックス 1 4 i の出力ビット数 (= 8) の半分 (= 4 ビット) とすることが好ましい。ここで、「等価的に」の語は、4 ビットシフトに代えて、例えば 1 2 (= 4 + 8 × 1) ビットシフト又は 2 0 (= 4 + 8 × 2) ビットシフトのように、出力ビット数の整数倍を加えた変形例（換言すると、出力ビット数 (= 8) で除算すると、余りが除数の半分 (= 4) のビット数となるシフト量をもつ変形例）を包含することを意味している。また、S ボックス 1 4 i の出力ビットは、1 2

ビットシフトされた場合には、SボックスS3、S4ではなく、SボックスS2、S3に反映され、20ビットシフトされた場合にはSボックスS1、S2に反映される。さらに、Sボックス14_iの出力ビットを2つのSボックスS3、S4（S2、S3又はS1、S2を含む）に反映させる場合、4ビットずつの組合せに限らず、順不同で1ビットと7ビット、2ビットと6ビットあるいは3ビットと5ビットの組合せとしてもよい。すなわち、等価的な4ビットシフトに代えて、等価的な1～3、5～7の任意のビットシフトとしてもよい。

【0061】

加算部16_iは、拡大変換部15_iから入力された12ビットの拡大変換結果と、一時鍵レジスタ11_i内の32ビットのデータからなる第2鍵KBとを加算し（桁上りを伴う通常の加算）、得られた加算結果をラウンドR_iの拡大鍵K_iとして攪拌部20のラウンド関数f_{ri}に入力する機能をもっている。

【0062】

なお、一時鍵レジスタ11_iから抽出される第1鍵KA及び第2鍵KBは、図2においては、それぞれ連続する領域から個別に取出されたが、これに限らず、不連続な領域から取り出してもよい。すなわち、第1鍵KAは、一時鍵レジスタ11_i内の任意の合計8ビットのデータであればよく、第2鍵KBは、一時鍵レジスタ11_i内の任意の合計32ビットのデータであればよい。また、第1鍵KAは、第2鍵KBと重なっていてもよい。なお、第1鍵KAのビット長は、攪拌部20のSボックスの入力ビット長と等しくすることがSボックスの共有化の観点から好ましい。第2鍵KBのビット長は、拡大鍵K_iのビット長と等しくすることが、設計の簡易化の観点から好ましい（但し、所望により、第2鍵KBと拡大鍵K_iのビット長を互いに異ならせてもよく、この場合、例えば縮約型転置や拡大転置等を用い、最終的に拡大鍵K_iのビット長を調整可能である）。

【0063】

巡回シフト部17_iは、一時鍵レジスタ11_iの値を所定のシフト量だけ巡回シフトさせて次段の一時鍵レジスタ11_{i+1}に入力するものであり、ここでは図5に示すように、各鍵変換関数f_{k1}～f_{kn}毎に、シフト量が設定されている。なお、巡回シフト部17_iのシフト量は、鍵の攪拌性を高める観点から、少な

くとも共通鍵 K_C のビット数又は S ボックス 14_i の出力ビット数のいずれかと互いに素であることが好ましく、三者が互いに素であることが最も好ましい。また、このシフト量は、拡大鍵 $K_1 \sim K_{16}$ を逆順 ($K_{16} \sim K_1$) にも生成可能とする観点から、最終段を除いた鍵変換関数 $f_{k1} \sim f_{k(n+1)}$ の中央値 ($n=8$) を中心として左右対称 (前段、後段で対称) に設定されている。但し、これに限らず、巡回シフト部 17_i は、拡大鍵 $K_1 \sim K_{16}$ を逆順 ($K_{16} \sim K_1$) にも生成可能であれば、シフト量及び巡回方向を任意に設定可能である。

【0064】

一方、攪拌部 20 は、夫々ラウンド R_1 からラウンド R_n までの n ラウンドの処理において、拡大鍵生成部 10 から順に拡大鍵 $K_1 \sim K_{16}$ が与えられるとき、入力された平文を暗号化して暗号文を出力する暗号化機能を有し、また、拡大鍵生成部 10 から暗号化とは逆順に拡大鍵 $K_{16} \sim K_1$ が与えられるとき、入力された暗号文を復号して平文を出力する復号機能を有している。攪拌部 20 には、各ラウンド $R_1 \sim R_n$ に対応して、順にカスケード接続されたラウンド関数 $f_{r1} \sim f_{rn}$ が設けられている。

【0065】

ラウンド関数 f_{ri} は、暗号化のとき、平文又は中間的な暗号化結果を、拡大鍵生成部 10 から入力された拡大鍵 K_i に基づいて変換し、中間的な暗号化結果又は暗号文を出力する関数であり、復号のとき、暗号文又は中間的な復号結果を、拡大鍵生成部 10 から逆順に入力された拡大鍵 $K_{(n+1-i)}$ に基づいて変換し、中間的な復号結果又は平文を出力する関数であって、ここでは一例として図 6 に示す如き Feistel 構造が使用されている。

【0066】

図 6 中の Feistel 構造は、与えられた 2 つのサブブロック L_i , R_i からなるデータブロックのうち、一方のサブブロック R_i を拡大鍵 K_i に基づいて F 関数で非線形変換し、この変換結果と他方のサブブロック L_i との排他的論理和を XOR 素子 21 で算出し、この算出結果 R_{i+1} と一方のサブブロック L_{i+1} ($=R_i$) との位置を交替して次段に与える、という構成を備えている。

【0067】

ここで、F関数は、図6中において、拡大鍵 K とサブブロック R_i （又は L_i ）との排他的論理和を算出するXOR素子22と、XOR素子22の出力を4分割して夫々非線形変換する4つのSボックス $S_1 \sim S_4$ とから構成される。

【0068】

なお、各ラウンド関数 f_r による変換は、同じ変換を2回繰り返すと、元のデータが復元されるインボルーション（involution）という性質をもっている。このため、攪拌部20では、平文を拡大鍵 $K_1 \sim K_{16}$ の順に変換して暗号文を生成したとき、この暗号文を拡大鍵 $K_{16} \sim K_1$ の順に再度変換すると、平文が生成可能となっている。

【0069】

次に、以上のように構成された暗復号装置の動作を説明する。

暗号化の際には、図1に示すように、入力された共通鍵 K_C 又は中間的な鍵変換結果 k_{ci} は、鍵変換関数 f_{ki} により1ラウンド毎に拡大鍵 K_i に変換される。

【0070】

詳しくは図7に示すように、鍵変換関数 f_{ki} においては、一時鍵レジスタ11_iから取り出した8ビットの第1鍵 K_A と定数レジスタ12_i内の定数との排他的論理和をXOR素子13_iが算出し、この算出結果をSボックス14_iが非線形変換する。非線形変換としては、例えば図4に示した関係で入力と出力とを各ビット毎に置換する。この置換結果は、拡大変換部15_iにより4ビット左シフト（＝16倍）されて加算部16_iに入力される。

【0071】

加算部16_iは、入力されたシフト結果と一時鍵レジスタ11_iから取り出した32ビットの第2鍵 K_B とを加算し、加算結果を32ビットの拡大鍵 K_i として攪拌部20に出力する。

【0072】

この拡大鍵 K_i においては、Sボックス14_iで変換された8ビットの第1鍵 K_A が、右（最下位桁）から5ビット目～12ビット目に位置する。このビット位置は、第3及び第4のSボックス S_3 、 S_4 への入力に対応する。従って、拡

大鍵生成部 10 の S ボックス 14_i による攪拌作用を攪拌部 20 の 2 つの S ボックス S3, S4 に反映でき、拡大鍵の攪拌性が向上されている。

【0073】

また、攪拌部 20 では、平文が、各ラウンド関数 $f_{r1} \sim f_{rn}$ 毎に各拡大鍵 $K1 \sim Kn$ に基づいて変換され、中間的な暗号化結果を経て最終的に暗号文に変換される。

【0074】

一方、復号の際には、拡大鍵生成部 10 においては、前述同様に共通鍵 K_C が入力されると、暗号化時とは逆順に鍵変換処理が行われ、拡大鍵 $Kn \sim K1$ が順次、攪拌部 20 に出力される。

【0075】

攪拌部 20 では、入力された暗号文が、暗号化時とは逆順の拡大鍵 $Kn \sim K1$ に基づいて変換され、中間的な復号結果を経て最終的に平文に変換される。

【0076】

上述したように本実施形態によれば、各鍵変換関数 $f_{k1} \sim f_{kn}$ としては、入力された鍵から得られた第 1 鍵 KA に基づいて S ボックス 14_i (置換テーブル) により変換処理を行い、加算部 16_i が、この S ボックス 14_i による変換結果を左シフトさせた値と、入力された鍵から得られた第 2 鍵 KB とに基づいて拡大鍵 $K1 \sim K16$ を算出する。

【0077】

このように、外部装置を付加しない簡易な構成を用いており、拡大鍵 K_i を生成する際に、置換テーブル (S ボックス 14_i) による非線形変換処理を行うため、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度を向上させることができる。

【0078】

また、各鍵変換関数 f_{ki} では、巡回シフト部 17_i が、入力された鍵を左 (又は右) に巡回シフトさせ、巡回シフトの完了した鍵を次ラウンドの鍵変換関数 $f_{k(i+1)}$ に入力するので、容易且つ確実に、各ラウンドに入力される鍵を互いに相違させることができる。

【0079】

さらに、巡回シフト部 17_i のシフト量としては、例えば、Sボックス 14_i の出力ビット数と互いに素な値とした場合、各ラウンド R1～Rnにおけるほぼ全ての第1鍵KAを互いに相違させることができ、前述した効果をより一層、容易且つ確実に得ることができる。

【0080】

さらに、各鍵変換関数 f_{ki} としては、拡大変換部 15_i が、Sボックス 14_i による変換結果を拡大変換させて加算部 16_i に入力するので、前述した効果に加え、第1鍵KAの攪拌作用を拡大鍵Kiの任意の領域に反映させることができる。

【0081】

また、拡大変換部 15_i による拡大変換としては、所定ビット数のシフトであるので、前述した効果を容易且つ確実に得ることができる。

【0082】

さらに、攪拌部 20 が、暗号化及び復号のための複数のSボックス S1～S4を有し、攪拌部 20 のいずれかのSボックスが、鍵変換関数 $f_{k1} \sim f_{kn}$ のSボックス 14_i と共有化されているので、装置規模の縮小化を図ることができる。

【0083】

また、各鍵変換関数 $f_{k1} \sim f_{kn}$ としては、拡大変換部 15_i が、Sボックス 14_i による変換結果を受けたとき、この変換結果のビット数の半分のビット数、あるいは半分のビット数に変換結果のビット数の整数倍を加えた値のビット数だけ、当該変換結果を左シフトさせて加算部 16_i に入力するので、第1鍵KAの攪拌作用を拡大鍵Kiにて左シフトさせた領域に反映させることができ、この場合、攪拌部 20 の複数のSボックス S3、S4に入力される領域に反映させることができるので、より一層、暗号強度の向上を図ることができる。

【0084】

(第2の実施形態)

図8は本発明の第2の実施形態に係る拡大鍵生成装置に適用される鍵変換関数

の構成を示すブロック図であり、図 2 と同一部分には同一符号を付してその詳しい説明を省略し、ここでは異なる部分についてのみ述べる。なお、以下の各実施形態も同様にして重複した説明を省略する。

【 0 0 8 5 】

すなわち、本実施形態は、第 1 の実施形態の変形例であり、拡大鍵の攪拌性のより一層の向上を図るものであり、具体的には図 2 に示すように、各鍵変換関数において、前述した定数レジスタ 1 2_i、XOR 素子 1 3_i、S ボックス 1 4_i 及び拡大変換部 1 5_i からなる変換要素が互いに並列に、一時鍵レジスタ 1 1_i と加算部 1 6_i との間に接続されている。

【 0 0 8 6 】

ここで、2 つの S ボックス 1 4_i は、1 種類で設けてもよく、又は複数の種類で設けてもよいが、複数の種類を用いる場合、共通鍵 K C に基づいて拡大鍵 K i を正順及び逆順の両方で生成可能とする観点から、前半の鍵変換関数 f k 1 ~ f k 8 と後半の鍵変換関数 f k 9 ~ f k 1 6 とでは中央 (f k 8, 9) から上下対称となるように種類が設けられることが好ましい。

【 0 0 8 7 】

また、2 つの拡大変換部 1 5_i は、互いに同一のシフト量とすることも可能であるが、2 つの S ボックス 1 4_i による攪拌効果をより広範囲に反映させる観点から、互いに異なるシフト量で S ボックス 1 4_i の出力を左シフトさせることが好ましい。この場合、例えば一方の拡大変換部 1 5_i を 4 ビットの左シフトとし、他方の拡大変換部 1 5_i を 2 0 ビットの左シフトとすると、第 1 鍵 K A の攪拌効果を攪拌部 2 0 の S ボックス S 1 ~ S 4 の全てに反映できるので好ましい。

【 0 0 8 8 】

以上のような構成によれば、第 1 鍵 K A による攪拌性をさらに向上できるので、第 1 の実施形態の効果に加え、拡大鍵 K i の攪拌性をより一層向上させることができる。

【 0 0 8 9 】

(第 3 の実施形態)

図 9 は本発明の第 3 の実施形態に係る拡大鍵生成装置の構成を示すブロック図

である。

本実施形態は、第 1 又は第 2 の実施形態の変形形態であり、一時鍵レジスタ 11_i 及び巡回シフト部 17_i に代えて、入力される共通鍵 KC 又は中間的な鍵 $k_{c1} \sim k_{cn-1}$ の各ビットを互いに非線形的に置換し、得られた中間的な鍵の一部を自己の段の XOR 素子 13_i 並びに加算部 16_i に入力すると共に、その中間的な鍵の全体を次段の置換処理部 $18_{(i+1)}$ に入力する置換処理部 18_i を備えている。

【0090】

各置換処理部 18_i は、共通鍵 KC に基づいて拡大鍵 K_i を正順及び逆順の両方で生成可能とする観点から、共通鍵 KC を正順に n 回置換した結果が元の共通鍵 KC に等しくなるように夫々設定され、且つラウンド数 $n = 16$ の場合の例を図 10 に示すように、暗号化の際には昇順に変換を行い、復号の際には降順に逆変換を行うように設定されている。

【0091】

以上のような構成としても、第 1 又は第 2 の実施形態と同様の効果を得ることができ、これに加え、容易且つ確実に、各鍵変換関数 $f_{k1} \sim f_{kn}$ に入力される鍵 KC 、 $k_{c1} \sim KC_{n-1}$ を互いに相違させることができる。

【0092】

なお、上記各実施形態では、S ボックス 14_i の入力側に、定数を排他的論理和する XOR 素子 13_i を設けた場合について説明したが、これに限らず、XOR 素子 13_i を省略し、S ボックス 14_i に代えて、定数の排他的論理和を算出した後の S ボックス 14_x を設けた構成としても、本発明を同様に実施して同様の効果を得ることができる。

【0093】

(第 4 の実施形態)

次に、本発明の第 4 の実施形態に係る暗復号装置について図 11 を用いて説明する。この暗復号装置 30 は、第 1 乃至第 3 の実施形態のいずれかで述べた構成を有し、例えば画像データや音楽データ等のデジタル情報（以下、生データという）を保護するためのものである。

【0094】

係る暗復号装置30は、例えば図11に示すように、記憶媒体からプログラムがインストールされることにより、パーソナルコンピュータ（以下、パソコンという）PCに実現されているとする。ここで、暗復号装置30は、例えばユーザIDを共通鍵とし、パソコンPCに入力された生データを暗号化し、得られた暗号化データ（前述した暗号文に相当）を携帯可能な記憶素子31に記憶させる。この種の記憶素子31としては、ICカード、スマートメディア又はメモリカードなどがある。

【0095】

この記憶素子31がユーザ宅へ配布され、ユーザ宅内の図示しない暗復号装置は、自己のユーザIDに基づいて記憶素子31内の暗号化データを復号し、得られた画像データや音楽データをスピーカ等から再生出力させる。これにより、例えば予め契約したユーザのみに生データ（コンテンツ）を配布することができる。

【0096】

また、本実施形態は、以下のように種々変形可能となっている。例えば、図12に示すように、パソコンPCに代えて、例えばハードウェア回路からなる暗復号装置30を備えた記録装置32を設けた構成である。この構成によれば、コンテンツを記憶素子31に書込む際に、暗復号装置30がユーザID等により生データを暗号化して記憶素子31に記憶させる。宅配から復号に至る過程は、前述した通りである。このように、パソコンPC等の汎用のコンピュータでなくとも、専用の記録装置32に暗復号装置30を設けた構成としてもよい。

【0097】

また、図13に示すように、暗復号装置30を設けたホストコンピュータ33が、ネットワークNWを介してパソコンPCに接続された構成としてもよい。この場合、ホストコンピュータ33からダウンロードされた暗号化データがパソコンPCを介して暗号化された状態で記憶素子32に記憶される。宅配から復号に至る過程は、前述した通りである。この変形例によれば、前述した効果に加え、ネットワークNW上でのコンテンツ（生データ）の盗聴などを防止することがで

きる。

【0098】

さらに、図14(a), (b)に示すように、記憶素子を例えばDVD (digital versatile disc) としてもよい。図14(a)に示す場合、予め暗号化データが格納されたDVD34がユーザに頒布される。ユーザ宅の暗復号装置30は、DVD34内の暗号化データを復号し、得られた画像データや音楽データをスピーカ等から再生出力させる。

【0099】

また、図14(b)に示す場合、画像や音楽等の生データがユーザ宅の暗復号装置30によって所定の共通鍵を用いて暗号化され、得られた暗号化データがDVD-RAM35に格納される。

この暗号化データは、ユーザにより設定された所定の共通鍵により復号されるが、共通鍵が知られない限り、他人には復号されない。従って、趣味的な画像データや音楽データなどを他人から保護しつつ保存することができる。

【0100】

(他の実施形態)

尚、本発明における拡大鍵生成装置及び暗復号装置の処理を実現させるためのプログラムが記憶された記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク(CD-ROM、CD-R、DVD等)、光磁気ディスク(MO等)、半導体メモリ等が適用可能である。実際には、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であっても良い。

【0101】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS(オペレーティングシステム)や、データベース管理ソフト、ネットワークソフト等のMW(ミドルウェア)等が本実施形態を実現するための各処理の一部を実行しても良い。

【0102】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、

LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0103】

また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も本発明における記憶媒体に含まれ、媒体構成は何れの構成であっても良い。

【0104】

尚、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であっても良い。

【0105】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0106】

また、本発明は、DES暗号系に限らず、ラウンド関数を用いるブロック暗号系であれば適用可能であり、例えば、Lucifer、LOKI、MISTY 1、MISTY 2 及び SAFER(Secure And Fast Encryption Routine) といった暗号系に適用してもよい。

【0107】

その他、本発明はその要旨を逸脱しない範囲で種々変形して実施できる。

【0108】

【発明の効果】

以上説明したように本発明によれば、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度を向上できる拡大鍵生成装置、暗復号装置及び記憶媒体を提供できる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施形態に係る暗復号装置の構成を示すブロック図

【図 2】

同実施形態における暗復号装置内の拡大鍵生成部の構成を示すブロック図

【図 3】

同実施形態における定数レジスタの設定値を説明するための模式図

【図 4】

同実施形態における S ボックスの構成を説明するための模式図

【図 5】

同実施形態における巡回シフト部の設定を説明するための模式図

【図 6】

同実施形態におけるラウンド関数の構造を示すブロック図

【図 7】

同実施形態における動作を説明するための模式図

【図 8】

本発明の第 2 の実施形態に係る拡大鍵生成装置に適用される鍵変換関数の構成を示すブロック図

【図 9】

本発明の第 3 の実施形態に係る拡大鍵生成装置の構成を示すブロック図

【図 1 0】

同実施形態における置換処理部の設定を説明するための模式図

【図 1 1】

本発明の第 4 の実施形態に係る暗復号装置を説明するための模式図

【図 1 2】

同実施形態における変形例を説明するための模式図

【図 1 3】

同実施形態における変形例を説明するための模式図

【図 1 4】

同実施形態における変形例を説明するための模式図

【図 1 5】

従来の共通鍵暗号の一例としてのDES方式を説明するためのブロック図

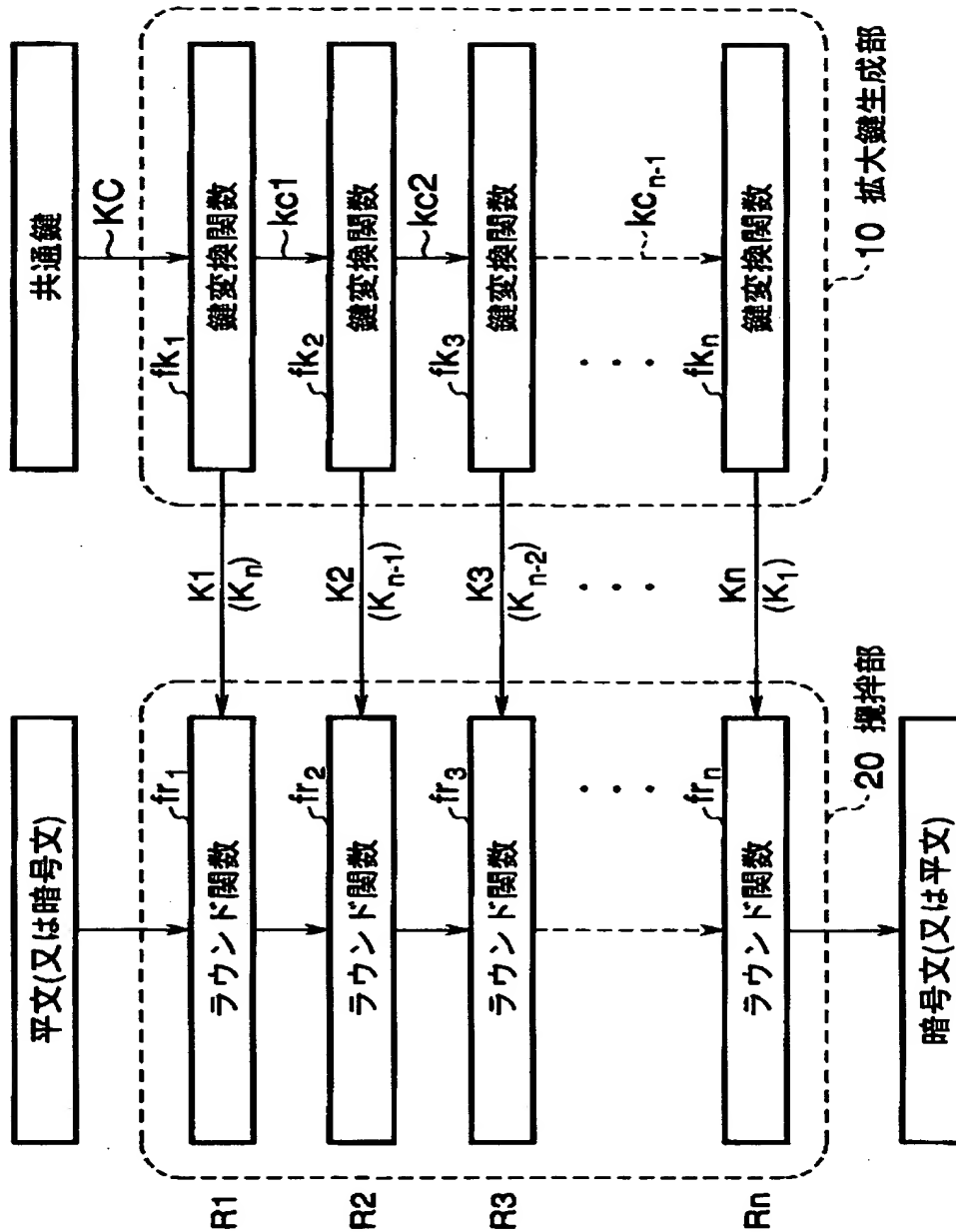
【符号の説明】

1 0 … 拡大鍵生成部
 1 1₁ ~ 1 1_n … 一時鍵レジスタ
 1 2₁ ~ 1 2_n … 定数レジスタ
 1 3₁ ~ 1 3_n … XOR素子
 1 4₁ ~ 1 4_n … Sボックス
 1 5₁ ~ 1 5_n … 拡大変換部
 1 6₁ ~ 1 6_n … 加算部
 1 7₁ ~ 1 7_{n-1} … 巡回シフト部
 1 8_i … 置換処理部
 2 0 … 攪拌部
 3 0 … 暗復号装置
 3 1 … 記憶素子
 3 2 … 記録装置
 3 3 … ホストコンピュータ
 3 4 … DVD
 3 5 … DVD-RAM
 f k 1 ~ f k n … 鍵変換関数
 R 1 ~ R n … ラウンド
 K 1 ~ K n … 拡大鍵
 K C … 共通鍵
 k c 1 ~ k c n-1 … 鍵変換結果
 K A … 第 1 鍵
 K B … 第 2 鍵
 P C … パソコン
 N W … ネットワーク

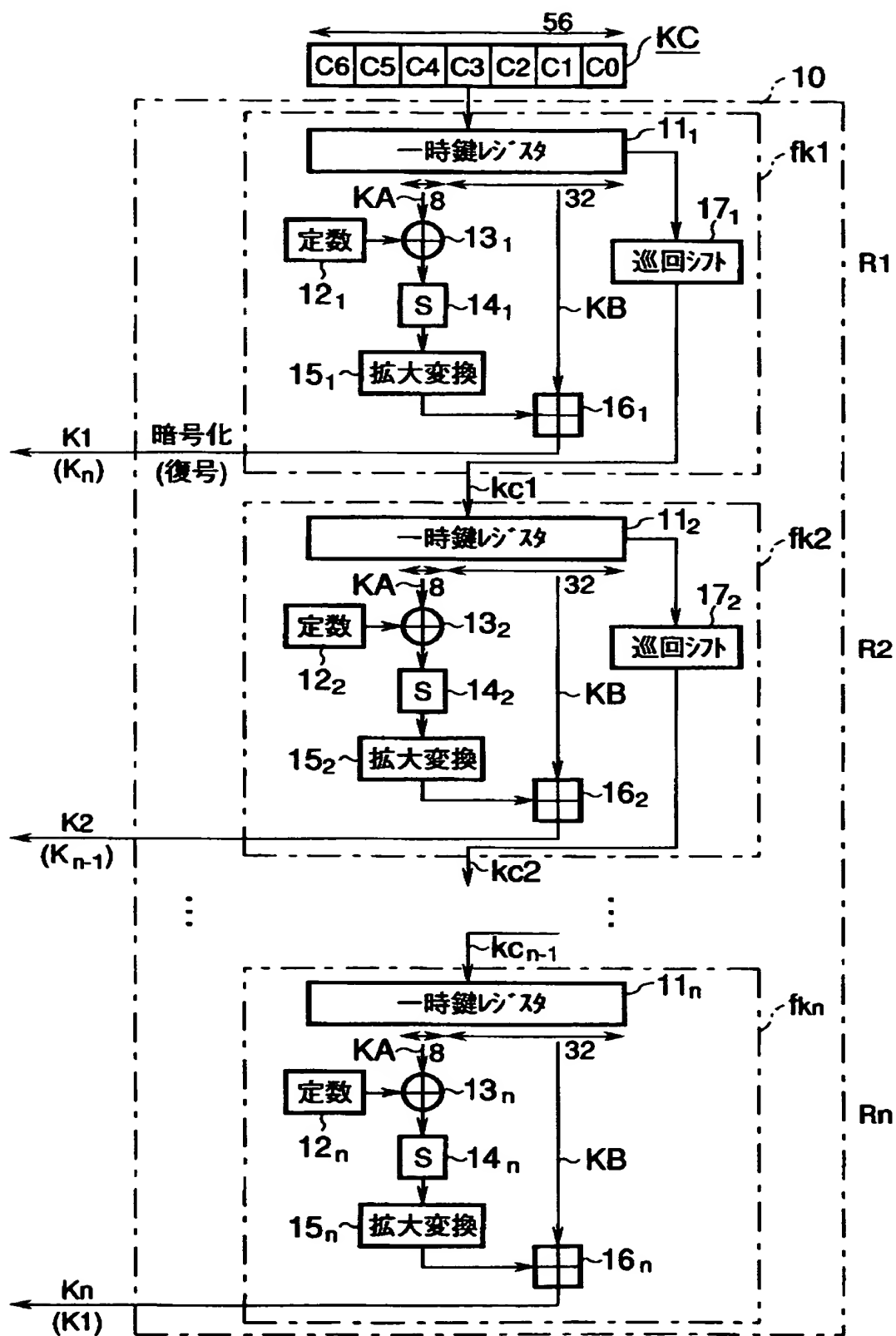
【書類名】

図面

【図 1】



【図 2】



【図 3】

鍵変換関数 <i>f</i> _k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
定数レジスタの値	0	1	2	3	4	5	6	7	7	6	5	4	3	2	1	0

(a)

鍵変換関数 <i>f</i> _k		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
定数レジスタ の値	暗号化	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	復号	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0

(b)

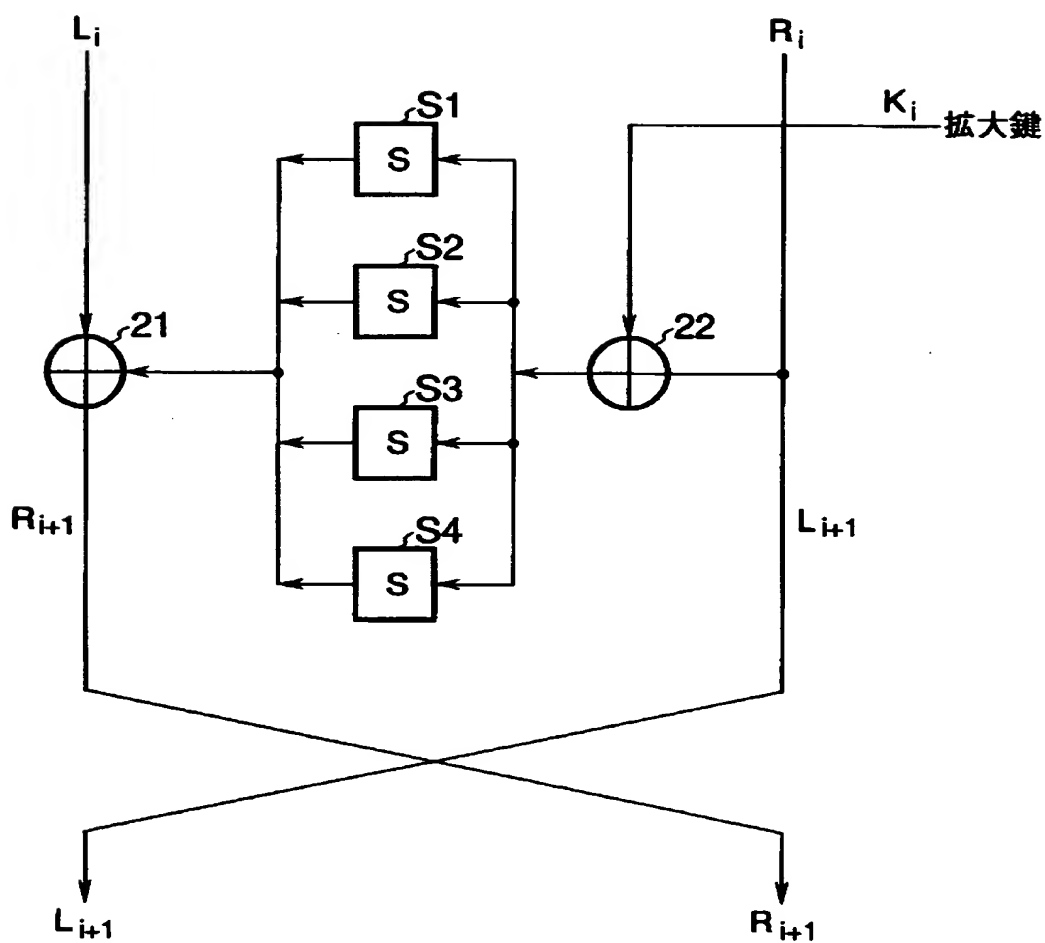
【図 4】

48,	54,	216,	182,	175,	5,	130,	229,	107,	52,	86,	11,	12,	221,	14,	15,
59,	4,	41,	140,	22,	164,	7,	89,	124,	81,	225,	176,	101,	66,	30,	118,
126,	242,	44,	211,	18,	161,	249,	105,	222,	174,	141,	202,	34,	103,	87,	233,
71,	49,	187,	51,	39,	1,	91,	77,	181,	172,	55,	42,	199,	79,	62,	194,
64,	72,	68,	133,	190,	158,	165,	232,	231,	115,	186,	116,	217,	240,	129,	171,
74,	169,	204,	173,	57,	58,	93,	17,	159,	245,	241,	155,	92,	156,	94,	26,
132,	82,	109,	230,	227,	28,	131,	209,	170,	25,	106,	73,	85,	98,	128,	143,
237,	108,	160,	61,	21,	179,	254,	197,	38,	122,	235,	70,	125,	31,	40,	102,
246,	119,	207,	53,	214,	111,	63,	135,	184,	236,	138,	56,	19,	29,	213,	88,
144,	145,	243,	127,	148,	137,	189,	151,	78,	153,	123,	183,	114,	157,	255,	252,
33,	6,	147,	163,	84,	97,	166,	167,	192,	0,	10,	208,	117,	196,	9,	16,
27,	206,	177,	104,	195,	83,	24,	75,	150,	203,	188,	50,	100,	69,	20,	180,
134,	193,	168,	8,	251,	247,	149,	201,	200,	112,	43,	142,	139,	205,	212,	37,
60,	226,	210,	154,	239,	80,	244,	215,	3,	120,	45,	23,	67,	99,	219,	223,
250,	220,	191,	32,	185,	253,	121,	13,	36,	228,	96,	162,	136,	46,	238,	146,
110,	178,	152,	2,	90,	234,	95,	65,	248,	113,	224,	35,	76,	218,	198,	47,

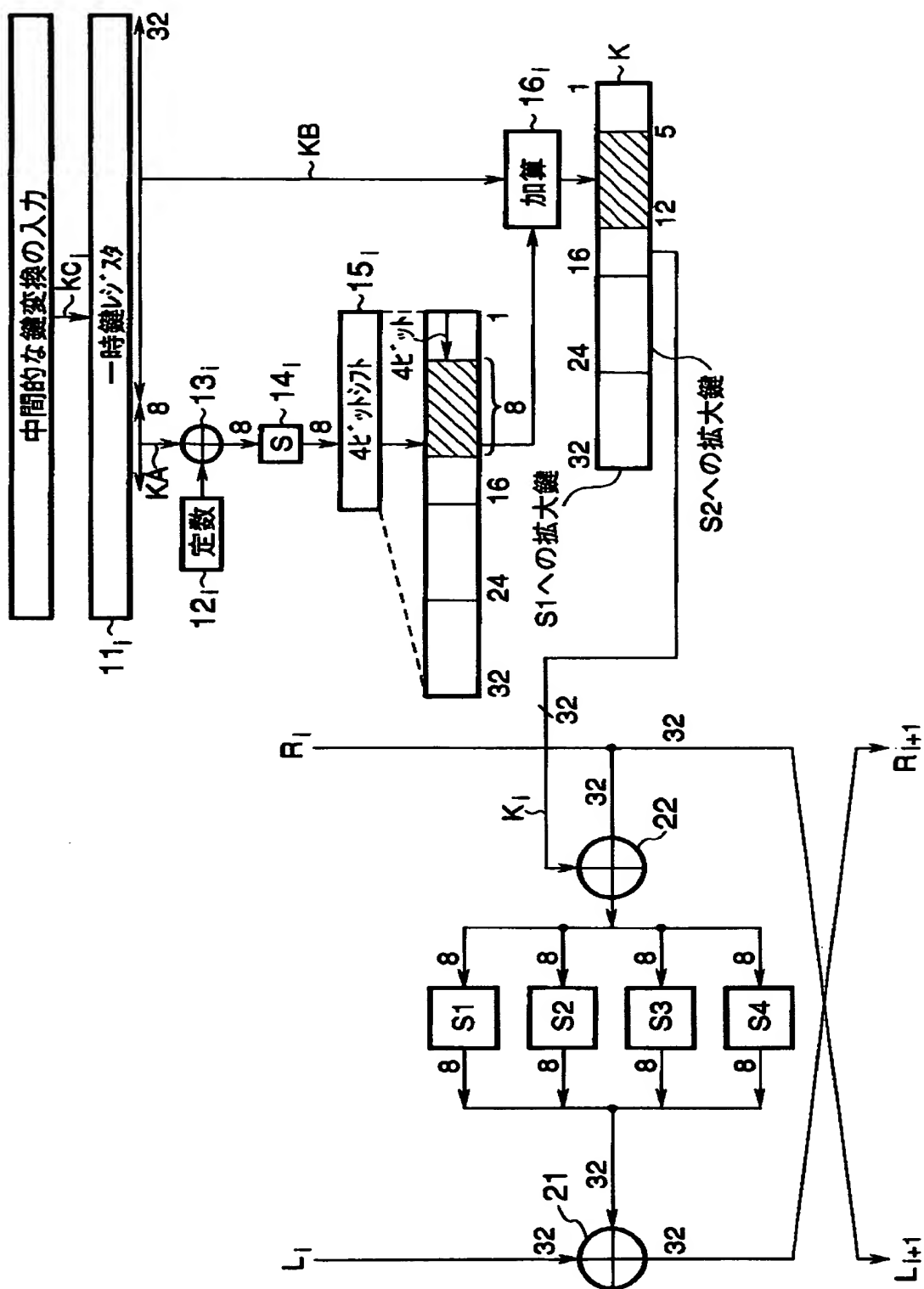
【図 5】

ラウンド数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
	暗号化(左巡回シフト)	9	9	11	11	13	13	13	10	13	13	13	11	11	9	9
復号(右巡回シフト)	9	9	11	11	13	13	13	13	10	13	13	13	11	11	9	9
鍵変換関数 <i>k_i</i>	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	15

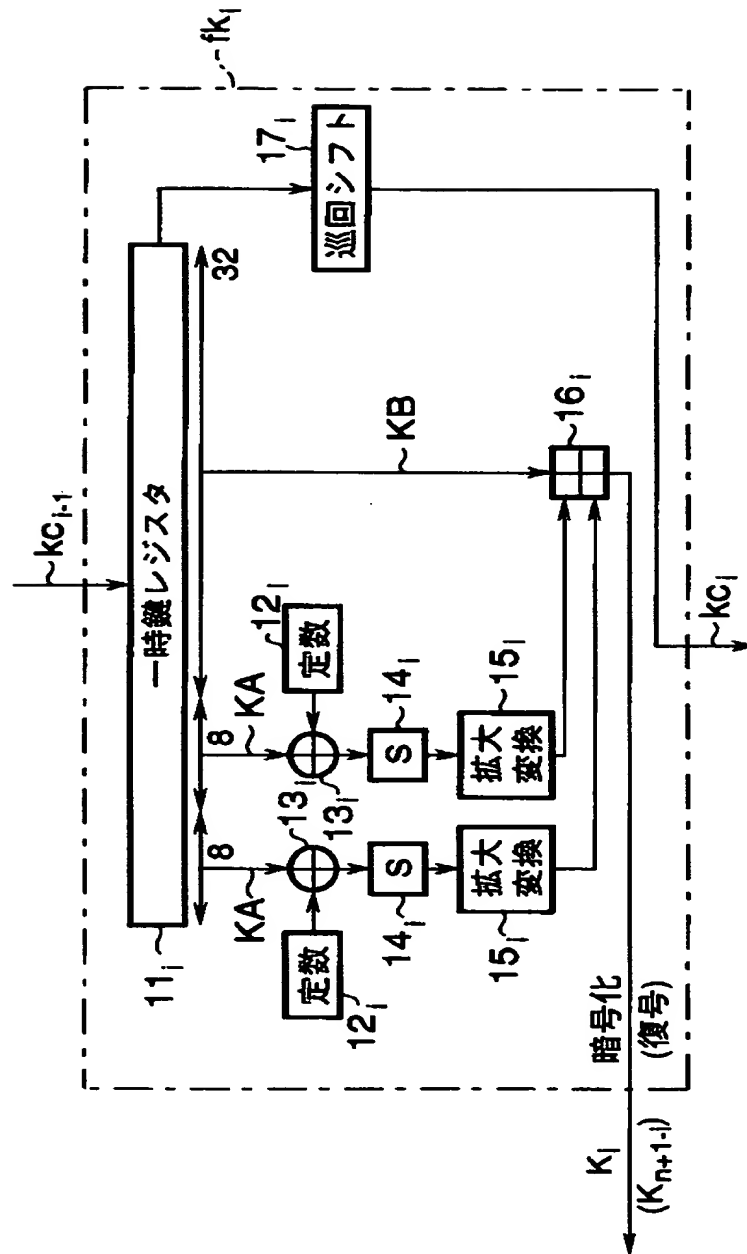
【図 6】



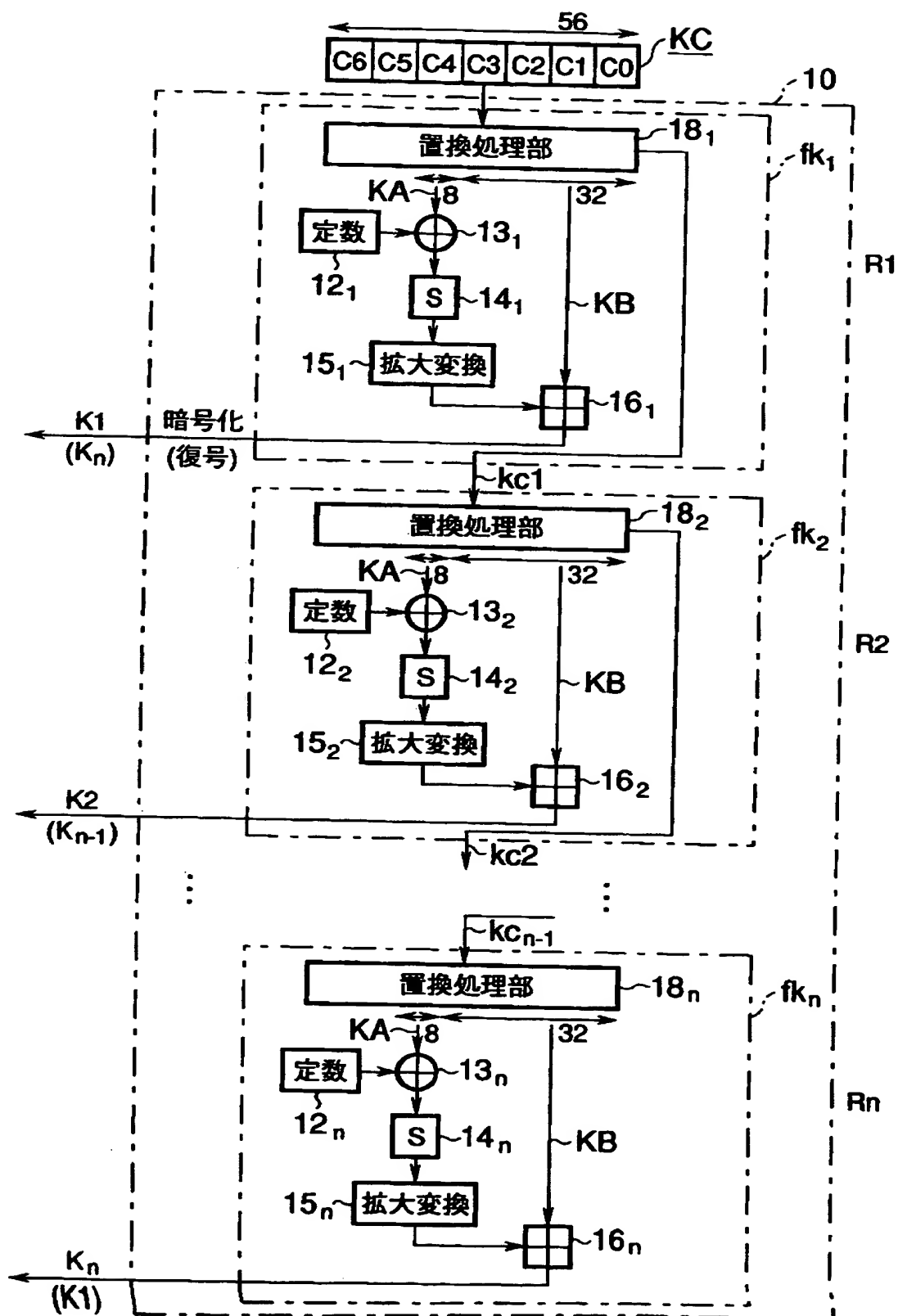
【图 7】



【図 8】



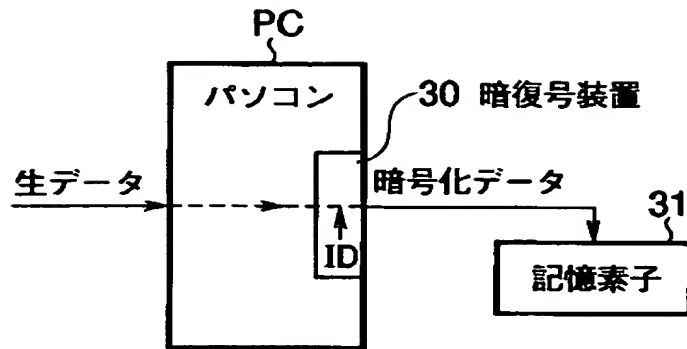
【図 9】



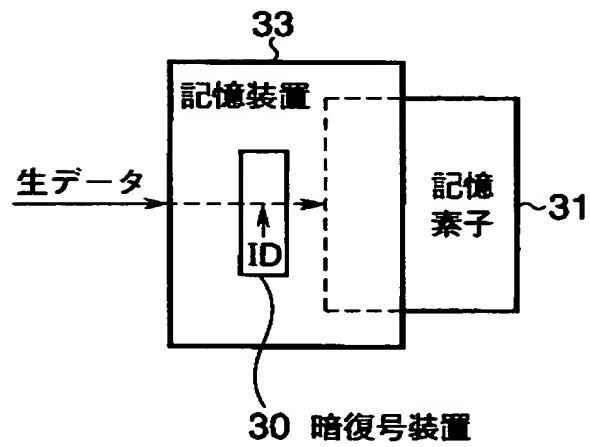
【図 1 0】

ラウンド数	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	
	暗号化	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14	P15	P16
転置入力 処理	復号	P16 ⁻¹	P15 ⁻¹	P14 ⁻¹	P13 ⁻¹	P12 ⁻¹	P11 ⁻¹	P10 ⁻¹	P9 ⁻¹	P8 ⁻¹	P7 ⁻¹	P6 ⁻¹	P5 ⁻¹	P4 ⁻¹	P3 ⁻¹	P2 ⁻¹	P1 ⁻¹

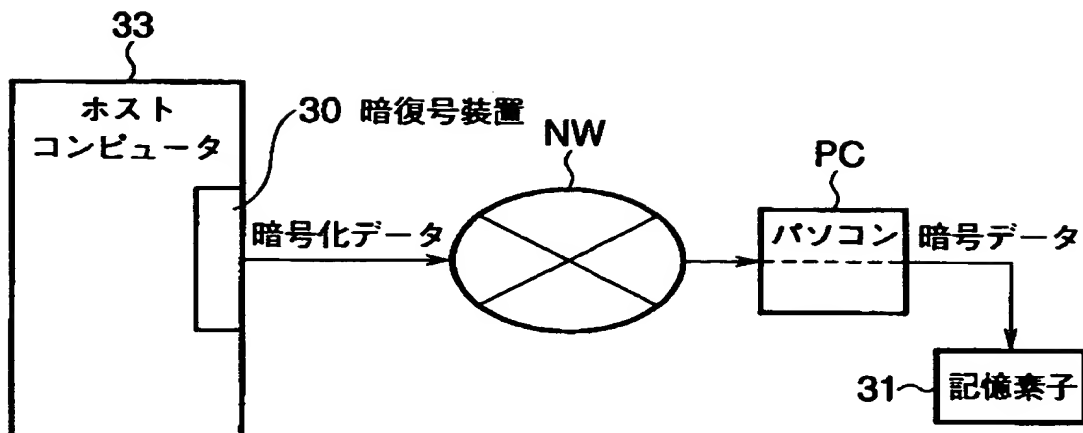
【図 1 1】



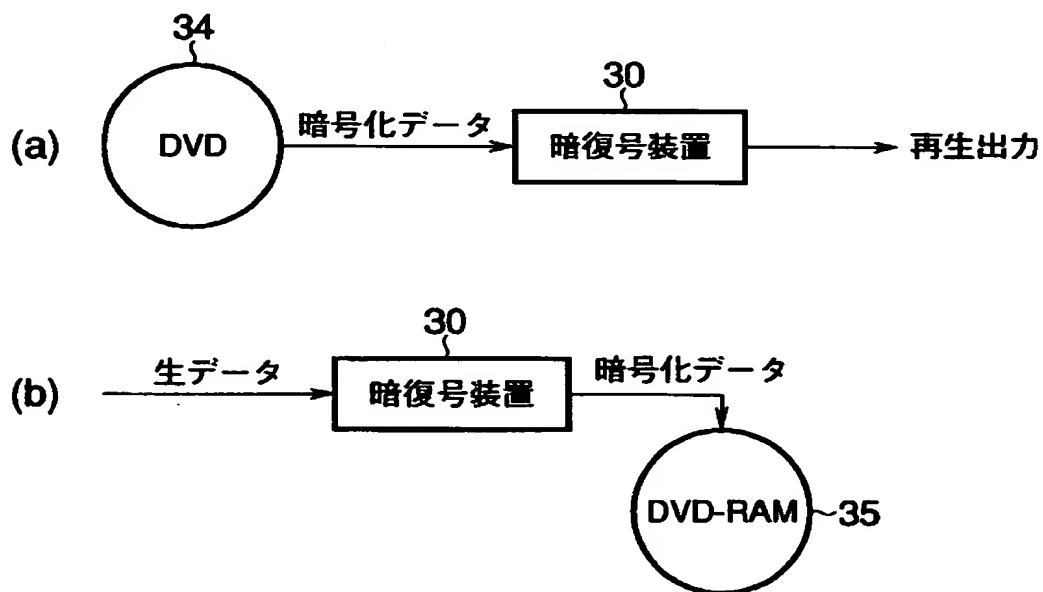
【図 1 2】



【図 1 3】



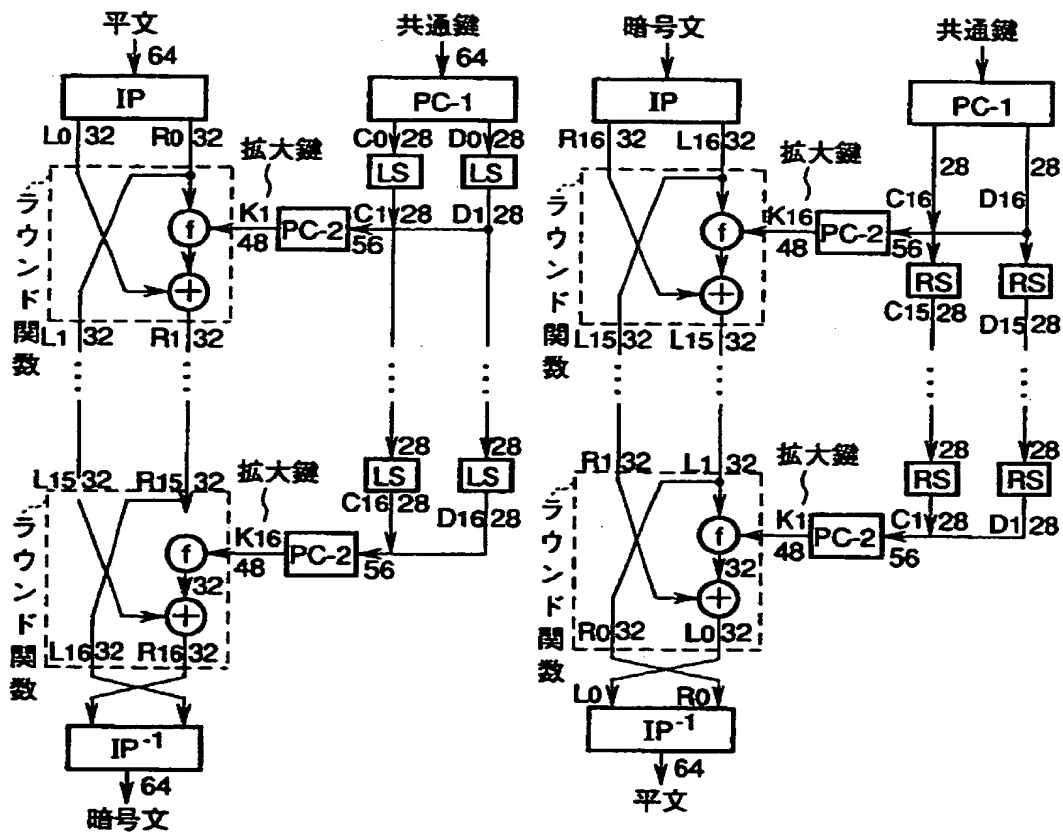
【図 1 4】



【図 1 5】

(a) DES暗号化

(b) DES復号化



【書類名】 要約書

【要約】

【課題】 本発明は、装置価格や装置規模を抑え、弱鍵の生成を阻止しつつ拡大鍵の攪拌性を向上でき、もって、暗号強度の向上を図る。

【解決手段】 各鍵変換関数 $f_{k1} \sim f_{kn}$ としては、入力された鍵から得られた第1鍵 KA に基づいて S ボックス 14_i (置換テーブル) により変換処理を行い、加算部 16_i が、この S ボックス 14_i による変換結果を左シフトさせた値と、入力された鍵から得られた第2鍵 KB とに基づいて拡大鍵 $K1 \sim K16$ を算出する拡大鍵生成装置、暗復号装置及び記憶媒体。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 5 8 2 1]

1. 変更年月日	1 9 9 0 年 8 月 2 8 日
[変更理由]	新規登録
住 所	大阪府門真市大字門真 1 0 0 6 番地
氏 名	松下電器産業株式会社

出 願 人 履 歴 情 報

識別番号 [0 0 0 0 0 3 0 7 8]

1. 変更年月日	1 9 9 0 年 8 月 2 2 日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町 7 2 番地
氏 名	株式会社東芝



Creation date: 06-29-2004
Indexing Officer: DGREEN - DONALD GREEN
Team: OIPEBackFileIndexing
Dossier: 09652157

Legal Date: 10-12-2000

No.	Doccode	Number of pages
1	CTMS	1

Total number of pages: 1

Remarks:

Order of re-scan issued on